Discrete Applied Mathematics 24 (1989) 153–165
North-Holland

FACTORISATIONS COURTES DANS UN GROUPE FINI*

Y.O. HAMIDOUNE
Université Pierre et Marie Curie, U.E.R. 48 – ER Combinatoire, 4 Place Jussieu, 75230 Paris Cedex, France

Received 27 October 1988

Let G be a finite group and let S be a generating subset of G. We give upper bounds for the minimum length of a sequence of elements of S whose product is a given element. Our bounds are reached.

Introduction

L'existence de factorisations courtes d'éléments d'un groupe fini est liée à une certaine décomposition d'un graphe de Cayley. Cette décomposition est valable pour une classe plus générale de graphes, notamment ceux dont le groupe d'automorphismes agit transitivement sur l'ensemble des sommets.

Après un rappel de notions élémentaires relatives aux graphes, nous définissons les atomes positifs. Nous donnons une nouvelle démonstration courte du fait que deux atomes positifs distincts sont disjoints. Cette propriété est essentielle pour la décomposition ci-dessus mentionnée. Nous présentons ensuite une synthèse des résultats utilisés pour la démonstration de l'existence de factorisations courtes.

1. Graphes

Nous rappelons dans cette section quelques définitions et propriétés élémentaires des graphes pour la commodité de lecteurs peu familiers avec ces notions.

Soient V et E deux ensembles, o et t deux applications de E vers V. On dit que $X=(V,E,o,t)$ est un graphe. Les éléments de E seront appelés arcs de X, ceux de V seront appelés sommets de X. Soit e un arc de X. On dit que $o(e)$ (respectivement $t(e)$) est l'origine (respectivement terminus) de e.

Généralement on représente les sommets par des points. Un arc est alors representé par une flèche reliant son origine à son terminus.

Un arc e tel que $o(e)=t(e)$ est appelé une boucle. Deux arcs e et e' tels que $o(e)=o(e')$ et $t(e)=t(e')$ seront dits parallèles. Un graphe sans boucles ni arcs

* Nous donnons une synthèse de résultats démontrés dans des articles antérieurs. Certaines démonstrations sont plus courtes que les originales.

parallèles est dit simple. Un graphe simple peut être défini par un couple (V,E), où V est un ensemble et $E\subset V\times V\setminus\{(x,x): x\in V\}$.

Soient X un graphe et x un sommet de X. On pose

$$\omega^+(x)=\{e\in E: o(e)=x\},\qquad \omega^-(x)=\{e\in E: t(e)-x\}.$$

Le demi-degré extérieur (respectivement intérieur) d'un sommet x est par définition

$$d^+(x)=|\omega^+(x)|\qquad (\text{respectivement } d^-(x)=|\omega^-(x)|).$$

Soit $A\subset V(X)$, on pose

$$N^+(A)-\{x\in V(X)-A: \exists e\in E(X),\ o(e)\in A \text{ et } t(e)=x\},$$

$$N^-(A)=\{x\in V(X)-A: \exists e\in E(X),\ t(e)\in A \text{ et } o(e)=x\}.$$

On écrira $N^+(x)$ au lieu de $N^+(\{x\})$, et de même pour $N^-(x)$.

Soit X un graphe simple. Alors $d^+(x)=|N^+(x)|$ et $d^-(x)=|N^-(x)|$.

Soit $X=(V,E,o,t)$ un graphe. Le graphe *inverse* de X est par définition le graphe $X^{-1}=(V,E,t,o)$. C'est le graphe obtenu en renversant les orientations de tous les arcs de X.

Soient X un graphe, x et y deux sommets de X. Soit $\mu=[e_1,e_2,\ldots,e_k]$ une suite d'arcs tels que

(1) $o(e_1)=x$ et $t(e_k)=y$,
(2) $\forall i,\ 1\le i\le k-1,\ t(e_i)=o(e_{i+1})$.

On dit que μ est un *chemin* reliant x à y. On admet un chemin vide reliant x à x. Un chemin tel que $\forall i,j,\ o(e_i)=o(e_j)\Rightarrow i=j$ est appelé un chemin élémentaire.

De tout chemin reliant x à y, on peut extraire un chemin élémentaire reliant x à y.

Un graphe où deux sommets quelconques sont reliés par un chemin est dit fortement connexe.

Soient $X=(V,E,o,t)$ un graphe et $A\subset V$. Le sous-graphe de X induit par A est par définition $X[A]=(A,F,o/F,t/F)$, où

$$F=\{e\in E: o(e)\in A \text{ et } t(e)\in A\}.$$

La relation "Il existe un chemin de X reliant x à y et un chemin reliant y à x" sera désignée par $x\phi y$.

ϕ est une relation d'équivalence sur V.

Une classe d'équivalence pour cette relation est appelée une composante fortement connexe de X.

Soit C une composante fortement connexe de X. Alors $X[C]$ est un graphe fortement connexe.

Un graphe est fortement connexe si et seulement si il possède une unique composante fortement connexe.

Soit X un graphe. Alors X^{-1} possède les mêmes composantes fortement connexes que X.

Tous les graphes considérés à partir de maintenant seront supposés simples et finis.

Une partie propre B de $V(X)$ est appelée un puits (respectivement une source) si $N^+(B)=\emptyset$ (respectivement $N^-(B)=\emptyset$).

Soit X un graphe qui n'est pas fortement connexe. Alors il existe deux composantes fortement connexes distinctes dont l'une est une source et l'autre un puits.

Un graphe X est fortement connexe si et seulement si pour toute partie propre A de $V(X)$, $N^+(A)\neq\emptyset$.

Soient X un graphe, x et y deux sommets de X, μ et μ' deux chemins reliant x à y. On dit que μ et μ' sont intérieurement disjoints si $V(\mu)\cap V(\mu')=\{x, y\}$, où $V(\mu)$ désigne l'ensemble des sommets de μ.

Soient X un graphe, x et y deux sommets de X. On dit qu'un sous-ensemble T de $V(X)-\{x, y\}$ sépare y de x si $X[V-T]$ ne contient aucun chemin reliant x à y. Autrement dit tout chemin reliant x à y passe par un sommet de T. Une condition nécessaire et suffisante pour l'existence d'un tel T est que $y\notin N^+(x)$ (par abus de language on dira que (x, y) n'est pas un arc de X). Plaçons nous dans ce dernier cas. La connectivité entre x et y est par définition

$$\kappa(x, y)=\mathrm{Min}(|T|: T \text{ sépare } y \text{ de } x).$$

Le nombre maximum de chemins de x vers y deux à deux intérieurement disjoints sera noté $\tau(x, y)$.

Supposons que (x, y) no soit pas un arc de X. On voit facilement que $\tau(x, y)\leq\kappa(x, y)$. L'inégalité inverse est moins évidente. Elle est l'object du théorème ci-dessous.

Théorème 1.1 (Menger 1927). *Soient x et y deux sommets d'un graphe X tels que $y\notin N^+(x)$. Alors $\tau(x, y)=\kappa(x, y)$.*

Le théorème de Menger entraîne très simplement le théorème de Ford–Fulkerson sur le flot maximum. On trouve une courte preuve du théorème de Menger dans [8].

Le graphe complet symétrique d'ordre n est un graphe X tel que $|V(X)|=n$ et $E(X)=\{(x, y): x\neq y \text{ et } x, y\in V(X)\}$.

Soit X un graphe fortement connexe et $T\subset V(X)$; on dit que T est un ensemble de séparation de X si $X-T=X[V-T]$ n'est pas fortement connexe. Il est clair que le graphe symétrique complet n'a pas d'ensemble de séparation. La forte connectivité d'un graphe X est

$$\kappa(X)=\begin{cases}|V(X)|-1, & \text{si } X \text{ est symétrique complet,}\\ \mathrm{Min}\{|T|: T \text{ est un ensemble de séparation de } X\}, & \text{autrement.}\end{cases}$$

$\kappa(X)$ est donc le nombre minimum de sommets qu'il faut supprimer pour rendre le graphe non fortement connexe si X n'est pas symétrique complet. Dans ce cas on a

$$\kappa(X)=\mathrm{Min}\{\kappa(x, y): x, y\in V(X),\ x\neq y \text{ et } (x, y)\notin E(X)\}.$$

Les deux résultats suivants se déduisent facilement de Théorème 1.1 et sont appelés théorèmes de Menger.

Théorème 1.2 (Menger). *Un graphe X est fortement k-connexe si et seulement si*

$$\forall x, y \in V(G), \quad x \neq y, \quad \tau(x, y) \geq k.$$

Théorème 1.3 (Menger). *Soient X un graphe fortement k-connexe, A et $B \subset V(X)$ tels que $|A|, |B| \geq k$. Alors il existe k chemins deux à deux disjoints reliant A à B.*

2. Atomes d'un graphe

Les atomes sont été utilisés dans le cas non orienté pour l'étude de la connectivité par Watkins [10] et Mader [6] indépendamment (1970). Les définitions dans le cas orienté ont été posées par Chaty [1].

Soient X un graphe, T un ensemble de séparation de X tel que $|T| = \kappa(X)$ et $H = X - T$. Puisque H n'est pas fortement connexe, il possède des puits et des sources.

Un puits P (respectivement une source) de H est appelé un *fragment positif* (respectivement *négatif*) de X.

On a $N_H^+(P) = \emptyset$ et $N_H(S) = \emptyset$, et $P \neq V - T$, $S \neq V - T$.

Notons qu'on n'admet $V - T$ ni comme source ni comme puits.

Il résulte que $N_X^+(P) = T$. Puisque $P \cup N^-(P) \subset P \cup T \neq V$, $N_X^+(P)$ est donc un ensemble de séparation. Puisque T est un ensemble de séparation de cardinal minimal, on a forcément $N_X^+(P) = T$. De même $N_X^-(S) = T$.

D'habitude on définit les fragments par cette dernière propriété comme suit: On dit que F est un fragment positif (respectivement négatif) de X si

(i) $|N^+(F)| = \kappa(X)$ (respectivement $|N^-(F)| = \kappa(X)$),
(ii) $F \cup N^+(F) \neq V(X)$ (respectivement $F \cup N^-(F) \neq V(X)$).

Notons qu'un graphe symétrique complet n'a pas de fragments.

Lemme 2.1. *F est un fragment positif de X si et seulement si F est un fragment négatif de X^{-1}.*

Si F est un fragment positif (respectivement négatif) de X, on note $\bar{F} = V - (F \cup N^+(F))$ (respectivement $\bar{F} = V - (F \cup N^-(F))$).

Notons que $(F, N^+(F), \bar{F})$ est une partition de $V(X)$.

Lemme 2.2 [2]. *Si F est un fragment positif de X, alors $\bar{F}$ est un fragment négatif. En outre on a $N^-(\bar{F}) = N^+(F)$ et $(\bar{F})^- = F$.*

Démonstration. Soit $x \in N^-(\bar{F}) \cap F$, $\exists y \in \bar{F}$ tel que $(x, y) \in E(X)$. Donc $y \in N^+(F)$, ce qui est absurde. On en déduit $N^-(\bar{F}) \subset N^+(F)$. Par ailleurs $\bar{F}$ est une source de $X[V - N^-(\bar{F})]$, d'où $N^-(\bar{F})$ est un ensemble de séparation. Le fait que $|N^1(F)| = \kappa(X)$ entraîne que $N^+(F) = N^-(\bar{F})$. Ceci suffit pour montrer que $\bar{F}$ est un fragment négatif. □

Un fragment positif (respectivement négatif) A tel qu'il n'existe aucun autre fragment positif ou négatif de cardinalité $< |A|$ est appelé un *atome positif* (respectivement *négatif*).

Remarque. Un graphe possède toujours un atome qui peut être positif ou négatif. Certains graphes possèdent plusieurs atomes positifs sans posséder d'atomes négatifs. D'autres graphes possèdent des atomes positifs et des atomes négatifs à la fois.

Lemme 2.3. *Soit X un graphe et A un atome positif de X. Alors $X[A]$ est fortement connexe.*

Démonstration. Soit $H = X[A]$. Supposons que H ne soit pas fortement connexe et soit P un puits de H. On a $N_X^+(P) \cap A = \emptyset$. D'où $N_X^+(P) \subset N_X^+(A)$. Ceci suffit pour montrer que P est un fragment positif de X, ce qui contredit la définition d'un atome.

Lemme 2.4. *X possède un atome positif de cardinal* 1, *si et seulement si* $\kappa(X) = \mathrm{Min}(d^+(x) : x \in V(X))$.

Proposition 2.5 [2]. *Soient $X = (V, E)$ un graphe fortement connexe, A un atome positif et F un fragment positif tels que $A \cap F \neq \emptyset$. Alors $A \subset F$. En particulier deux atomes positifs distincts sont disjoints.*

Démonstration. Posons $T = N^+(A)$ et $S = N^+(F)$ (Fig. 1). $N^+(A \cap F)$ sépare $A \cap F$

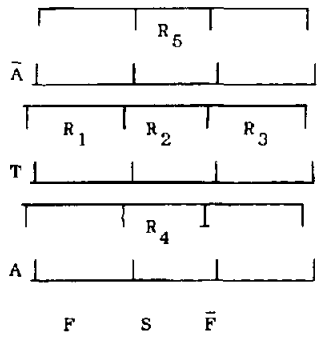

Fig. 1.

de $\bar{A}$. Donc $|N^+(A\cap F)|\geq\kappa(X)$. Par suite

$$|R_1|+|R_2|+|R_4|\geq|N^+(A\cap F)|\geq\kappa(X)=|R_1|+|R_2|+|R_3|.$$

D'où $|R_4|\geq|R_3|$. Maintenant

$$|\bar{F}-\bar{A}|=|\bar{F}\cap A|+|R_3|\leq|\bar{F}\cap A|+|R_4|<|A|.$$

Donc $\bar{F}\cap\bar{A}\neq\emptyset$, sinon on aurait un fragment $\bar{F}$ de cardinal $<|A|$. Mais $N^-(\bar{A}\cap\bar{F})$ sépare $\bar{A}\cap\bar{F}$ de A. D'où

$$|R_5|+|R_2|+|R_3|\geq|N^-(\bar{A}\cap\bar{F})|\geq|R_5|+|R_2|+|R_4|.$$

D'où $|R_3|\geq|R_4|$. Donc $|R_3|=|R_4|$. Par suite

$$|N^+(A\cap F)|\leq|R_1|+|R_2|+|R_4|=|R_1|+|R_2|+|R_3|=\kappa(X).$$

Donc $|N^+(A\cap F)|=\kappa(X)$. Il résulte que $A\cap F$ est un fragment positif. D'où $A\cap F=A$. □

La démonstration ci-dessus est plus simple que celle donnée dans [2]. Ce résultat dans le cas d'un graphe symétrique équivaut à un théorème de Mader [6]. Le fait que deux atomes distincts sont disjoints a été démontré dans le cas d'un graphe symétrique par Watkins [10].

3. Atomes d'un graphe sommet-transitif

Les graphes considérés ici sont supposés simples. L'isomorphisme entre deux graphes peut donc être défini de la manière suivante: Soient X, Y deux graphes et $f: V(X)\to V(Y)$. On dit que f est un *isomorphisme* de X sur Y si f est bijective et si en outre on a

$$\forall x,y\in V(X),\quad (x,y)\in E(X)\ \Leftrightarrow\ (f(x),f(y))\in E(Y).$$

Le groupe d'automorphismes de X se note $\mathrm{Aut}(X)$.

On dit que X est *sommet-transitif* lorsque le groupe d'automorphismes de X opère transitivement sur l'ensemble des sommets.

Proposition 3.1 [2]. *Soient X un graphe sommet-transitif et A un atome positif de X. Alors $X[A]$ est un graphe sommet-transitif. Si B est un autre atome positif de X, alors $X[B]$ est isomorphe à $X[A]$. En outre les atomes positifs de X forment une partition de $V(X)$.*

Démonstration. Soient x et y deux sommets de $X[A]$. Il existe un automorphisme f de X tel que $f(x)=y$. Puisque $f(A)\cap A\neq\emptyset$ on a $f(A)=A$. Ceci suffit à montrer que f/A est un automorphisme de $X[A]$.

Soient $x \in A$ et $y \in B$. $\exists f \in \mathrm{Aut}(X)$ tel que $f(x)=y$. Puisque $f(A) \cap B \neq \emptyset$. On a $f(A)=B$. Ceci suffit à montrer que f/A est un isomorphisme de $X[A]$ sur $X[B]$.

Pour montrer que les atomes positifs de X forment une partition de $V(X)$, il suffit de voir que $\forall x \in V(X)$, il existe un atome positif de X contenant x, car les atomes positifs sont deux à deux disjoints. Soit $x \in X$ et $a \in A$, $\exists f \in \mathrm{Aut}\, X$, tel que $f(a)=x$, d'où $x \in f(A)$ qui est manifestement un atome positif de X.

Ce résultat a été démontré dans le cas d'un graphe symétrique par Watkins [10]. □

Proposition 3.2 [4]. *Soit X un graphe sommet-transitif et A un atome positif de X. Alors $|A| \leq \kappa(X)$.*

Démonstration. Considérons le graphe Y obtenu de X en supprimant tous les arcs intérieurs aux atomes positifs. Soient x et y deux sommets de X. Il existe deux atomes positifs A et B tels que $x \in A$ et $y \in B$. Mais $X[A]$ et $X[B]$ sont isomorphes, d'où $d^-_{X[A]}(x) = d^+_{X[B]}(y)$. Il résulte que

$$d^+_Y(x) = d^+_X(x) - d^+_{X[A]}(x) = d^+_X(y) - d^+_{X[B]}(y) = d^+_Y(y).$$

De même on a $d^-_Y(x) = d^-_Y(y)$. Y est donc régulier. Soit m le nombre d'arcs de Y reliant A à $N^+(A)$:

$$m = r \cdot |A| \leq r \cdot |N^+(A)| = r \cdot \kappa(X),$$

où $r = d^+(Y)$. D'où $|A| \leq \kappa(X)$.

Proposition 3.3 [4]. *Soit X un graphe sommet-transitif fortement connexe. Alors $\kappa(X) \geq [\frac{1}{2} d^+(X)] + 1$.*

Démonstration. Soit A un atome de X, que nous supposons positif quitte à considérer X^{-1} qui est sommet transitif et de même connectivité.

Soit $x \in A$, on a $N^+(x) \subset (A - x) \cup N^+(A)$, d'où $d^+(x) \leq 2\kappa(X) - 1$. Donc $\kappa(X) \geq [\frac{1}{2} d^+(X)] + 1$. □

Proposition 3.4 [4]. *Soit X un graphe sommet-transitif anti-symétrique fortement connexe. Alors*

$$\kappa(X) \geq [\tfrac{2}{3} d^+(X)] + 1.$$

Démonstration. Les notations sont celles de la démonstration de Proposition 3.3.

D'après Proposition 3.1, $X[A]$ est régulier. D'où $d^+(X[A]) < \frac{1}{2}|A|$, sinon on aurait un arc symétrique.

$$d^+(x) \leq d^+(X[A]) + \kappa(X) < \tfrac{1}{2}|A| + \kappa(X).$$

D'où $d^+(X) < \frac{3}{2}\kappa(X)$. D'où $\kappa(X) \geq [\frac{2}{3} d^+(X)] + 1$. □

4. Diamètre d'un graphe sommet-transitif

Le diamètre d'un graphe X est la distance maximale entre un couple de sommets. On la note $\delta(X)$.

$$\delta(X) = \mathrm{Max}\{\mathrm{dist}(x, y): x, y \in V(X)\}.$$

Lemme 4.1 [3]. *Soit X un graphe fortement connexe régulier. Alors*

$$|V(X)| \geq \kappa(X)(\delta(X) - 3) + 2d^+(X) + 2.$$

Démonstration.

Cas 1: $\delta(X) \geq 3$. Soient x et y deux sommets tels que $\mathrm{dist}(x, y) = \delta(X) = t$. Posons $\kappa(X) = k$. Il existe k chemins deux à deux intérieurement disjoints (μ_i) $1 \leq i \leq k$ reliant x à y. Chacun de ces chemins est de longueur $\geq t$.

Nous allons supposer en plus que $\sum_{i=1}^{k} |V(\mu_i)|$ est minimal. Il résulte que

$$|V(\mu_i) \cap N^+(x) = 1 \quad \text{et} \quad V(\mu_i) \cap N^-(y)| = 1, \quad 1 \leq i \leq k.$$

$$|N^+(x) \cup N^-(y) - \bigcup V(\mu_i)| \geq 2d^+(X) - 2k.$$

D'où

$$|V(X)| \geq |N^+(x) \cup N^-(y) - \bigcup V(\mu_i)| + \sum_{1 \leq i \leq k} (|V(\mu_i)| - 2) + 2.$$

Par suite

$$|V(X)| \geq 2d^-(X) - 2k + k(t-1) + 2 \geq 2d^+(X) + k(t-3) + 2.$$

Cas 2: $\delta(X) = 2$. Soient A un atome de X, $x \in A$. Nous supposerons A positif quitte à remplacer X par X^{-1}. On a clairement

$$d^+(x) \leq |A| - 1 + \kappa(X) \leq \tfrac{1}{2}(n - \kappa(X)) - 1 + \kappa(X).$$

D'où $n \geq 2d^+(X) - \kappa(X) + 2$, où $n = |V(X)|$. □

Lemme 4.1 a été montré dans le cas symétrique par Watkins [9]. Lemme 4.1 et les résultats sur la connectivité des graphes sommet-transitifs permettent d'obtenir facilement les résultats suivants:

Proposition 4.2 [3] *Soient X un graphe sommet-transitif fortement connexe tel que $|V(X)| = n$ et $d^+(X) = r$. Alors*

$$\delta(X) \leq \frac{n + 1 - 2r + 3[\frac{1}{2}r]}{[\frac{1}{2}r] + 1}.$$

Proposition 4.3 [3]. *Soient X un graphe fortement connexe sommet-transitif antisymétrique. Alors*

$$\delta(X) \leq \left[\frac{n + 1 - 2r + 3[\frac{2}{3}r]}{[\frac{2}{3}r] + 1} \right].$$

Nous verrons que ces bornes sont atteintes par des graphes de Cayley.

5. Maille d'un graphe sommet-transitif

Rappelons que la maille d'un graphe X notée $g(X)$ est la cardinalité minimale d'un circuit de X.

Proposition 5.1 [3]. *Soit $X=(V,E)$ un graphe sommet-transitif. Alors $|V|\geq d^+(X)(g(X)-1)+1$. En particulier $g(X)\leq \lceil |V|/d^+(X)\rceil$.*

Démonstration. Supposons le contraire et soit X un contre-exemple de cardinal minimal. Posons $d=d^+(X)$, $n=|V|$ et $g=g(X)$. On a

$$n\leq d(g-1), \quad \text{d'où } g\geq 3.$$

Supposons que X ne soit pas fortement connexe. Soit C une composante fortement connexe qui est un puits. On a $d^+(X)=d^+(C)$. On vérifie facilement que C est sommet-transitif.

$$|V|>|C|\geq d^+(C)(g(C)-1)+1\geq d^+(X)(g-1)+1,$$

ce qui est absurde.

X est donc fortement connexe. Soit A un atome de X. On peut le supposer positif, quitte à passer par X^{-1} (qui a la même maille et le même degré). Montrons que $|A|\neq 1$.

Supposons $|A|=1$. Alors $\kappa(X)=d^+(X)$. Soient $x\in V$, $N^+(x)\cap N^-(x)=\emptyset$, car $g\geq 3$.

Par le théorème de Menger, il existe d chemins (μ_i), $1\leq i\leq d$ deux à deux disjoints reliant $N^+(x)$ à $N^-(x)$. Mais

$$|V(\mu_i)|\geq g-2.$$

On a donc

$$n=|V|\geq 1+\sum_{i=1}^{d}|V(\mu_i)|\geq 1+d(g-1),$$

une contradiction.

Donc $|A|\geq 2$. Mais $X[A]$ est sommet-transitif. Soit $r=d^+(X[A])$. Compte tenu de la minimalité de $|V|$, on a

$$(1) \qquad |A|\geq r(g(X[A])-1)+1\geq r(g-1)+1.$$

Soit $x\in A$, $T=N^+(A)$, $B=N^+(x)-A$.

Nous montrons les points suivants:

$$(2) \qquad N^-(x)-(A\cup T)\neq\emptyset.$$

Supposons le contraire. $N(x)\cup N^+(x)\subset A\cup T$. Par suite $2d=d^+(x)+d^-(x)\leq |A|+\kappa(X)\leq 2\kappa(X)$, ce qui contredit $|A|\geq 2$ compte tenu de Lemme 2.4. Soit $z\in N^-(x)-A\cup T$.

(3) Considérons le graphe $D=X-(T-B)$ et soit $b=|B|$. $\kappa(D)\geq\kappa(X)-|T|+|B|=b$. D'après le théorème de Menger, il existe donc b chemins deux à deux disjoints sauf en z, reliant B à z. Ces chemins ne peuvent pas rencontrer A, car $N_D^+(A)=B$. Il existe donc b chemins μ_i, $1\leq i\leq b$, deux à deux disjoints reliant B à $N(N(x)-A)$. Prenons ces chemins tels que $\sum_{i=1}^{b}|V(\mu_i)|$ soit minimal.

On a donc $N^-(x)\cap\bigcup_i V(\mu_i)=\emptyset$. On a donc

$$|V-A|\geq|N^-(x)-A|+\sum_{i=1}^{b}|V(\mu_i)|.$$

Mais $|V(\mu_i)|\geq g-2$.

Observons que

$$|N^+(x)-A|=d-d^+(A)=d-d^-(A)=|N^-(x)-A|=b.$$

Mais

$$\begin{aligned}|V-A|&\geq|N^-(x)-A|+b(g-2)\\&=|N^+(x)-A|+b(g-2)=b+b(g-2)=b(g-1).\end{aligned}$$

D'où

$$\begin{aligned}|V|&\geq|A|+|V-A|\geq r(g-1)+1+b(g-1)\\&=(r+b)(g-1)+1-d(g-1)+1.\end{aligned}$$ □

6. Graphes de Cayley

Soient G un groupe, que nous supposerons fini et $S\subset G-1$. Le graphe de Cayley défini par S est par définition

$$L(G,S)=(G,E)\quad\text{où}\quad E=\{(x,y):x^{-1}y\in S\}.$$

On a

$$N^-(x)=x.S=\{xs:s\in S\}.$$

Soit $\gamma_a:x\to ax$, $a\in G$, une translation à gauche. On a

$$(x,y)\in E\leftrightarrow x^{-1}y\in S\leftrightarrow(ax)^{-1}(ay)\in S\leftrightarrow(\gamma_a(x),\gamma_a(y))\in E.$$

Ceci suffit pour montrer que les translations à gauche sont des automorphismes de $L(G,S)$. En particulier $L(G,S)$ est sommet-transitif.

Il résulte donc qu'il existe un atome de $L(G,S)$ contenant 1.

Soit $x\in G$. Une factorisation de x suivant S est une suite $\{s_i:1\leq i\leq k\}$ d'éléments de S telle que $x=\prod_{1\leq i\leq k}s_i$, k est la longueur de la factorisation.

Lemme 6.1. *Soit G un groupe, $S\subset G-1$ et $x\in G$. Une factorisation de $x-\prod_{1\leq i\leq k}s_i$*

définit un chemin de longueur k de 1 *à x et inversement tout chemin de* 1 *à x définit une factorisation de x suivant S.*

Démonstration. Posons $x_0=1$, $x_j=\prod_{1\le i\le j} s_i$. Soit $x=\prod_{1\le i\le k} s_i$. Puisque $x_{j-1}=x_j s_{j+1}$, (x_j, x_{j+1}) est un arc. Donc $(x_0,x_1)(x_1,x_2)\dots(x_{k-1},x_k)$ est bien un chemin reliant 1 à x.

Soit $(1,x_1)(x_1,x_2)\dots(x_{k-1},x_k)$ un chemin reliant 1 à x. On a $x_{i+1}=x_i s_{i+1}$, où $s_{i+1}\in S$, $x=x_k=(x_{k-1})s_k$. Ceci entraîne que $x=\prod_{i=1}^{k} s_i$. □

Lemme 6.2. *$L(G,S)$ est fortement connexe si et seulement si S est un ensemble générateur de G.*

Démonstration. Supposons $L(G,S)$ fortement connexe et soit $x\in G$. Il existe un chemin reliant 1 à x. D'où l'existence d'une factorisation $x=s_1 s_2\dots s_k$, où $s_i\in S$, $1\le i\le k$. S est donc un ensemble générateur.

Supposons que S soit un ensemble générateur. Soit $x\in G$. Il existe une suite $(t_i)_{1\le i\le k}$, $t_i\in S\cup S^{-1}$ telle que $x=\prod_{1\le i\le k} t_i$.

Si $t_i\in S^{-1}$, posons $t_i=s^{-1}$. Puisque G est supposé fini, il existe p tel que $s^p=1$. On a donc $t_i=s^{-1}=s^{p-1}$.

En changeant tous les $t_i\in S^{-1}$ par des expressions de la forme s^{p-1}, où $s\in S$, on obtient une factorisation de x suivant S. Il suffit de remplacer x par $x^{-1}y$ pour compléter la démonstration. □

Proposition 6.3. *Soit A l'atome de $L(G,S)$ contenant* 1. *Alors A est sous groupe de G engendré par $S\cap A$.*

Démonstration. Soient $x, y\in A$. On a $xy\in\gamma_x(A)$, qui est un atome de même signe que A. Mais $x\in A\cap\gamma_x(A)$. D'où $A=\gamma_x(A)$ et par suite $xy\in A$.

Le reste résulte du fait que A est fortement connexe. □

7. Factorisations courtes

Proposition 7.1 [3]. *Soient G un groupe finit d'ordre n, $S\subset G$. Alors il existe une factorisation de l'unité de longueur $\le\lceil n/s\rceil$, où $s=|S|$.*

Démonstration. Le résultat est évident si $1\in S$. Supposons $1\notin S$. D'après ce qui précède un circuit C de G définit une factorisation de 1 de même longueur que $|C|$.

D'après Proposition 5.1, il existe un circuit de $L(G,S)$ de longueur $\le\lceil n/s\rceil$. □

Exemple 1 [3]. Soient $G=\mathbb{Z}_n$ et $S=\{1,2,\dots,s\}$, $s<\frac{1}{2}n$. On voit facilement que toute factorisation de 0 est de longueur $\ge\lceil n/s\rceil$. Ceci montre que la borne de Proposition 7.1 (et de Proposition 5.1) est la meilleure possible sans restriction sur S ou sur G.

Proposition 7.2 [3]. *Soient G un groupe d'ordre n, $S \subset G-1$ un ensemble générateur de cardinal s. Soit $x \in G-1$. Alors il existe une factorisation de x suivant S de longueur*

$$\leq \left\lfloor \frac{n+1-2s+3[\frac{1}{2}s]}{[\frac{1}{2}s]+1} \right\rfloor.$$

La démonstration résulte de Proposition 4.2 et de Lemme 6.1.

Exemple 2 [3]. Soient $G = \mathbb{Z}_m \times \mathbb{Z}_q$, $q > 3$, $S = \mathbb{Z}_m \times \{0,1\} - (0,0)$. On voit facilement que toute factorisation de $(0, q-1)$ est de longueur $\geq q-1$.

Mais $s = 2m-1$, $n = mq$. La borne de Théorème 7.2 est:

$$\frac{mq+1-2(2m-1)+3[2m-\frac{1}{2}]}{1+[2m-\frac{1}{2}]} = \frac{mq+3-4m+3(m-1)}{m} = q-1.$$

Proposition 7.3 [3]. *Soient G un groupe d'ordre n et $S \subset G-1$ un ensemble générateur de cardinal s tel que $S \cap S^{-1} = \emptyset$. Soit $x \in G-1$. Alors il existe une factorisation de x de longueur*

$$\leq \left\lfloor \frac{n+1-2s+3[\frac{2}{3}s]}{[\frac{2}{3}s]+1} \right\rfloor.$$

La démonstration résulte de Proposition 4.3 et de Lemme 6.1.

Exemple 3 [3]. $G = \mathbb{Z}_{2q+1} \times \mathbb{Z}_m$, $S = \{1, \ldots, q\} \times \{0\} \cup \mathbb{Z}_{2q+1} \times \{1\}$, $m > 2$.

On voit facilement que toute factorisation de $(0, m-1)$ a une longueur $\geq m-1$. Mais la borne de Théorème 7.2 ($S \cap S^{-1} = \emptyset$) est $m-1$.

Addendum

Bien après la rédaction de cet article, nous nous sommes aperçu que nos méthodes permettent de retrouver certains énoncés de la théorie additive combinatoire des nombres. C'est ainsi que le théorème de Cauchy–Davenport peut être obtenu à partir de Proposition 2.5.

Les cas $G = \mathbb{Z}_n$ et $G = \mathbb{Z}_n^*$ de Proposition 7.1 avaient été démontrés par Shepherdson (1947), cf. J. London Math. Soc. 22 (1947) 85–88. Le cas où G est abélien de Proposition 7.1 vient d'être redécouvert par Alon, cf. J. Number Theory 27 (1987) 196–205. Nous avons réussi à affiner nos méthodes afin de montrer un nouveau théorème d'addition généralisant le théorème de Cauchy–Davenport, un théorème de Shepherdson et un théorème d'Alon. Ces résultats seront publiés ailleurs.

Bibliographie

[1] G. Chaty, On critically and minimally k-vertex (arc) strongly connected digraphs, Proc. Keszthely (1971) 193–203.
[2] Y.O. Hamidoune, Sur les atomes d'un graphe orienté, C.R. Acad. Sci. Paris A 284 (1977) 1253–1256.
[3] Y.O. Hamidoune, An application of connectivity theory in graphs to factorization of elements in groups, European J. Combin. 2 (1981) 349–355.
[4] Y.O. Hamidoune, On the connectivity of Cayley digraphs, European J. Combin. 5 (1984) 309–312.
[5] Y.O. Hamidoune, Quelques problèmes de connexité dans les graphes orientés, J. Combin. Theory Ser. B. 30 (1981) 1–10.
[6] W. Mader, Über den Zusammenhang symmetricher Graphen, Arch. Math. 21 (1970) 331–336.
[7] W. Mader, Eine Eigenschaft der Atome endlicher Graphen, Arch. Math. 22 (1971) 333–336.
[8] McCuig, A short proof to Menger theorem, J. Graph Theory 8 (1984) 427–429.
[9] M.E. Watkins, Amer. Math. Monthly 74 (1967) 297.
[10] M.E. Watkins, Connectivity of transitive graphs, J. Combin. Theory 8 (1970) 23–29.